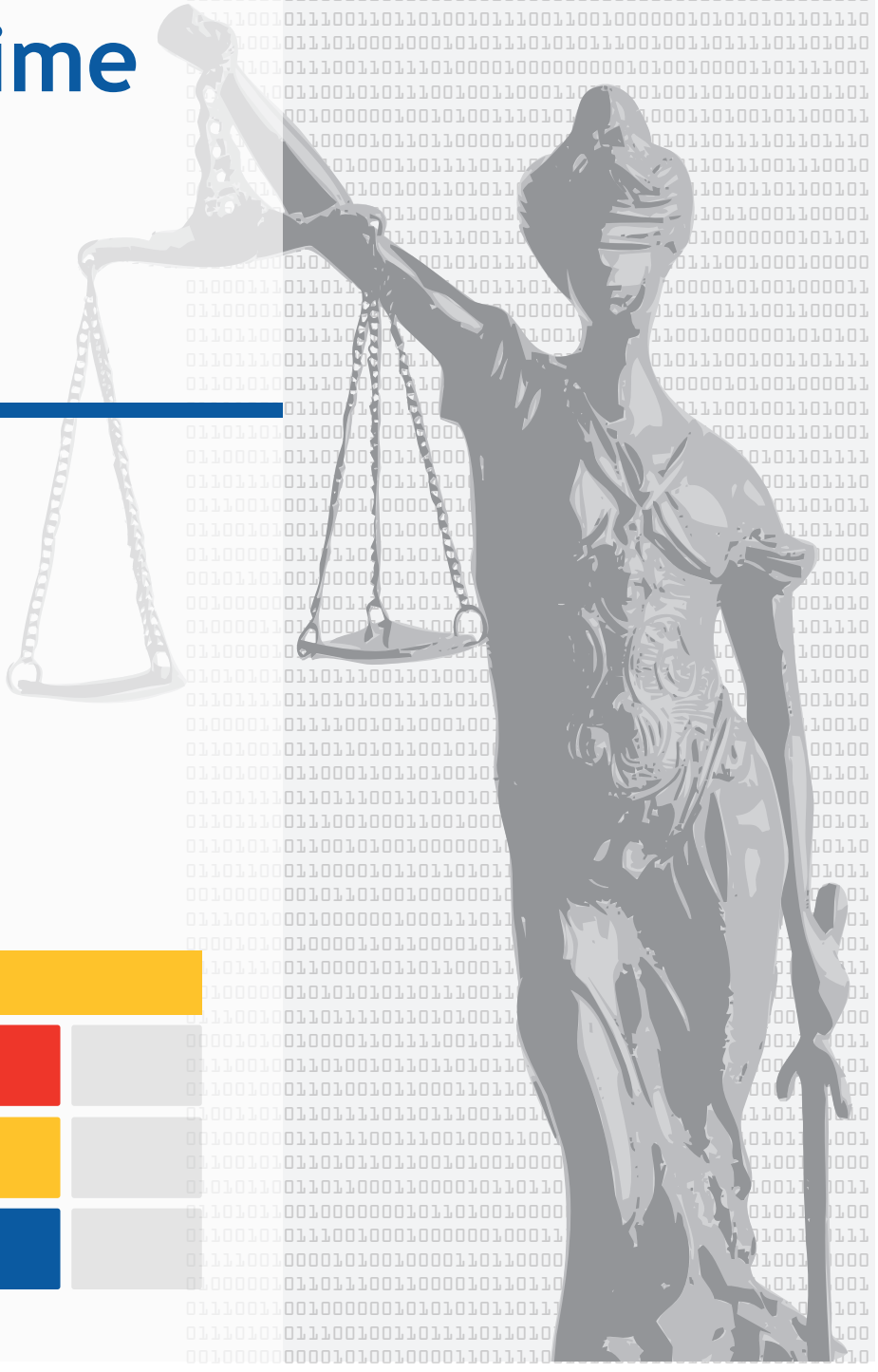
Cybercrime Judicial Monitor

Issue 2 - November 2016



Contents

1. Introduction

In this issue of the Cybercrime Judicial Monitor (CJM), three main sections are elaborated. In the first section on legislation an overview is given on the legislative developments which took place in 2016 in the area of cybercrime, cyber-related matters and electronic evidence.

The judicial analysis section presents legal analyses of several court decisions rendered by courts in The Netherlands, Italy, Spain and Ireland in cases concerning phishing with the use of malware; the admissibility of evidence gathered on the basis of remote access by installing a technical tool on a device; and the requirements for a judicial order authorising remote access or interception of communication, especially with regard to, for example, the right to privacy. In addition, summaries of other interesting court decisions that have been rendered in Europe are presented. The last part of this section focusses on the case of *Microsoft Corporation v. United States of America*. An analysis of the Court of Appeals ruling is presented, followed by a breakdown of the relevant legal provisions of the United States in relation to disclosure of data by service providers.

The subject of 'remote access to a computer system for the purpose of criminal investigations' has been selected as topic of interest for this CJM. In this section, a general overview is given of the legal landscape in relation to countries' possibilities to conduct remote access, with a distinction made according to the location of the accessed data. This overview is followed by an outline of the relevant legal provisions by country.

2. Legislation

The objective of this section is to provide information on recent developments in international, EU and national legal instruments in relation to cybercrime and e-evidence in 2016. The main sources of the information presented in this section are the contributions collected through the European Judicial Cybercrime Network, unless specifically stated otherwise.

2.1. EU level

European Commission

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

Source: Official Journal of the European Union

On 12 July 2016 the Commission adopted an implementing decision for the purpose of Article 25(2) of Directive 95/46/EC which sets general rules for transfers of personal data from Member States to third States. This decision establishes that the United States (U.S.) ensures an adequate level of protection for data transferred from the European Union to organisations in the U.S., allowing in this way such transfers to take place.

The most recent Privacy Shield scheme has been drafted to comply with the judgment of the Court of Justice of the European Union in the case of *Schrems*, which annulled the 'Safe Harbour' Decision, and addressed privacy concerns raised by the Commission. In doing so, the Decision provides a detailed review of the relevant rules of law in force in the United States. Furthermore, it provides an enhanced framework for the secure transfer of data as well as better and more transparent privacy policies from data operators.

Under the new scheme, in order to transfer data from European customers to the United States, organizations commit to a set of privacy principles, namely the EU – U.S. Privacy Shield Framework Principles together with the Supplemental Principles – issued by the U.S. Department of Commerce. This enhanced set of principles requires, firstly, that companies handling data under the Privacy Shield must face regular updates and reviews from the U.S. Department of Commerce with a view to assessing their adherence to the rules. Additionally, the conditions relating to onward transfers of data or third parties have been strengthened.

Secondly, clearer safeguards and transparency obligations on access by the U.S. government are in force. The U.S. has ruled out indiscriminate mass surveillance and has provided for such measures – if used – to be targeted and proportional. Furthermore, the U.S. Secretary of State

has created a redress possibility for Europeans affected by such government measures through an Ombudsperson mechanism at the Department of State.

Thirdly, the protection of individual rights has been strengthened by allowing for affordable and accessible dispute resolution mechanisms. Ideally, it is the organizations themselves that should provide a first avenue of redress. If this is not the case, free alternative dispute resolution (ADR) solutions will be offered together with the possibility to raise complaints locally with the Data Protection Authorities. The latter will, in turn, liaise with the Federal Trade Commission which will be able to investigate and help resolve the matter.

Fourthly, an annual joint review mechanism is set which will monitor the functioning of the Privacy Shield with involvement from the European Commission and the U.S. Department of Commerce, together with national security experts from the U.S. and European Data Protection Authorities.

The implementing decision has entered into force upon its communication to the Member States on 12 July 2016. Once companies have had the opportunity to review and update their compliance with the new scheme, registration will be available with the U.S. Department of Commerce starting 1 August 2016.

2.2. Member States

Austria

Amendments to §§ 117c, 118a ,126a and 126b of the Austrian Penal Code

On 1 January 2016, certain amendments to the Austrian Penal Code, mandated by Directive 2013/40/EU on attacks against information systems, came into force.

Pursuant to these amendments, cyberbullying – understood as persistent harassment involving telecommunications or a computer system – was criminalised. Furthermore, the amended criminal code has expanded criminal liability for the unlawful use of a computer system to also encompass "botnetting". Furthermore, a special provision was inserted which covers the situation where the offence involves a significant component of critical infrastructure.

Additionally, new provisions on damage to electronic data and on the disruption of the operation of a computer system were enacted. The amendment entails the punishment of the interference with multiple computer systems through the use of software or other means. In this latter situation, the amended criminal code prescribes a more stringent punishment where the offence caused damage exceeding 300000 Euro, interfered with essential elements of critical infrastructure or involved membership by the perpetrator in a criminal association.

Belgium

Statute of 29 May 2016 concerning the Collection and Retention of Data in the Electronic Communications Sector, introducing a new Article 126 to the Belgian Electronic Communications Statute.

On 29 May 2016 a new regime on the collection and retention of data came into force. This framework was introduced through Article 126 of the Belgian Electronic Communications Statute after the previous article on the issue was annulled by the Belgian Constitutional Court.

ISPs are obliged to retain subscriber and traffic data from their customers for a period of 12 months and are required to store it on the territory of the EU. Furthermore, the data has to be accessible from Belgium by the competent authorities. Law enforcement can only access the data when it meets the conditions laid down in Article 46bis C.P.C. (subscriber data) and Article 88bis C.P.C. (traffic data). Additionally, any access to the data has to be confined to a specialized Judicial Compliance Unit within the ISP, which has special security clearance for this purpose. Every access to such data needs to be logged by the service provider.

As far as crimes punishable with no more than one year custodial sentence, any production order for subscriber data is limited to the past six months and has to be issued by the prosecutor. Concerning traffic data, a production order needs to be warranted by an investigating judge and cannot be issued for crimes with a maximum sentence of one year or less. For crimes with a maximum sentence up to five years, such an order can only retrieve data from the past six months. Information from the past nine months can be retrieved for crimes punishable with more than five years in jail, while an order for the full 12 months can only be issued if it relates to terrorist crimes.

Special provision is made for lawyers and doctors whose professional privileges need to be respected.

France

Law nr. 2016-731 of 3 June 2016 reinforcing the fight against organized crime and terrorism and their financing, and improving the efficiency and safeguards provided in the Code of Criminal Procedure.

New legislation was enacted amending certain provisions of the Code of Criminal Procedure, which affords more powers of investigation to the competent authorities by allowing new ways of collecting e-evidence and accessing data stored on devices.

In particular, a judge may order law enforcement authorities, upon request by the prosecutor and without the knowledge of the suspect, to obtain remote access to communications stored on a device, for certain types of offences.

Greece

Legal provision 4411/2016 of 8 March 2016 transposing Directive 2013/40/EU on attacks against information systems.

The Convention on Cybercrime of the Council of Europe was ratified.

The Criminal Code was amended through the introduction of provisions on the obstruction of the operation of, and illegal access to, information systems as well as fraud using a computer and 'electronic data wear'. Also, a provision was included on grooming.

Ireland

Criminal Justice Bill 2016 - Offences relating to Information Systems.

A bill which transposes Directive 2013/40/EU on attacks against information systems is currently at the first stage of reading before the Parliament. A timeframe concerning the second stage of reading remains to be set.

Lithuania

Amended Article 198² of the Criminal Code relating to unlawful Handling of Equipment, Software, Passwords, Codes and other Data.

Article 198² of the Criminal Code which imposes a criminal penalty on any person who unlawfully handles equipment, software, passwords, codes and other data which are designed or adjusted for commission of criminal offences, was expanded in scope by providing a more detailed list of alternative punishable actions. Furthermore, a more stringent maximum sanction of four years of imprisonment instead of three was introduced.

The Netherlands

Legislative proposal 'Law on Computer criminality III' introducing a new Article 126nba Code of Criminal Procedure on remote access to a computer system.

A legislative proposal is currently being discussed, inserting a new Article 126nba in the Code of Criminal Procedure which will allow for remote access to a computer system -not being an extended search- through the use of a technical tool which is installed on the suspect's device from a distance. This technical possibility will allow key logging, copying files from the hard drive, and switching on or off the webcam or microphone of the device.

Source*: CJM questionnaire and Rijksoverheid.nl*

Poland

Law of 10 June 2016 on combating terrorism.

A new law came into force obliging users to register personal data when using pre-paid cards. ISPs providing internet access are required to verify the data before allowing access. This legal tool will make it more difficult for individuals to hide their identity when using pre-paid cards for internet access.

Additionally, certain amendments were made to legal provisions concerning investigative activities -description of procedures, registration process, internal supervision and control by the court- and usage of telecommunications data.

Romania

Articles 152, 154 and 168 of the Criminal Procedure Code.

The Code of Criminal Procedure has been amended to allow criminal investigation bodies, with prior authorisation from the Judge for Rights and Liberties, to request traffic and location data processed by service providers. This request can be made if, firstly, reasonable suspicion exists that a certain type of offence has been committed. Secondly, justified reasons need to be provided that the data constitutes evidence. Thirdly, the evidence cannot be obtained in any other way. Lastly, the request for the data needs to be a proportionate restriction of fundamental rights having regard to the details of the case at hand.

Furthermore, the amended Code provides that if reasonable suspicion exists regarding the preparation or commission of an offence, if collecting evidence is necessary or if a perpetrator, suspect or defendant has to be identified, then a prosecutor can order the preservation of computer data – including traffic data. Such data can be preserved when stored by service providers and when there is danger that it might be lost or altered. The same power applies if the data is stored on a computer system within the control of other persons.

Additionally, the Code now provides that computer searches can be conducted by specialized police officers in the presence of the prosecutor or of criminal investigation bodies.

Slovak Republic

Modifications of the Act 300/2005 Coll. (Criminal Code) as amended, to transpose Directive 2013/40/EU on attacks against information systems. Sections 247 to 247d C.C.

The amendment includes the criminalisation of unauthorized access to a computer system with more stringent punishment in case significant damage was caused therefrom or the perpetrator was part of a dangerous group. Also, the amendment criminalizes the restriction, limitation or interruption of the functioning of a computer system as well as the unauthorised interference

with, or interception of computer data. Furthermore, the amendment criminalizes the manufacturing and possession of a device – including computer software – as well as of a computer password which affords unauthorised access to a computer system.

Amendment of the Act 301/2005 Coll. (Code of Criminal Procedure). Sections 362f and 362g C.P.C.

Slovak law now provides for certain procedural rules to be followed before the Supreme Court in order to review the legality of an order to intercept and record (data on) telecommunication operation.

Amendment of the Act 171/1993 Coll. on the Police Forces. Section 76a, par.3

Act No. 171/1993 Coll. on the Police Forces was amended to the effect that Police are authorized to collect certain types of data in relation to a number of crime types.

Amendment of the Act 652/2004 Coll. on State administration authorities in customs as amended. Section 58, par. 2 and 3

The amendment introduced the obligation for service providers to provide certain types of data to customs authorities.

Act No. 351/2011 Coll. on electronic communications. Sections 58, 63 and 78c

Act No. 351/2011 Coll. on electronic communications was amended to the effect that private operators have the obligation to preserve or record certain types of data upon a positive authorisation by a court. Furthermore, private operators are obliged to produce such data upon a duly served request by the competent authorities.

2.3. Third States

Norway

Amendment to the Criminal Procedure Act introducing several coercive measures, including sections 126 o) and 126 p) on remote access to a computer system.

On June 17, 2016 the Criminal Procedure Act was amended providing for the legal bases for remote access by law enforcement authorities to a computer system. It is expected that the rules will be adopted this autumn.

When the amendments come into force, permission to remotely access computer systems can be given when someone is suspected of any criminal act punishable by law with a 10 year imprisonment or more.

United States of America

Amendment to Rule 41 of Rules of Criminal Procedure regarding the issuance of warrants.

Rule 41 of Rules of Criminal Procedure generally limits the issuance of a search warrant geographically. A recent amendment to Rule 41 of Rules of Criminal Procedure, allows a magistrate judge to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside their judicial district if the district where the information is located has been concealed through technological means or in an investigation into a violation of the computer damage statute where the damage involves computers in five or more districts. This amendment will go into effect on 1 December 2016 unless the U.S. Congress passes a law to prevent its implementation.

3. Judicial Analysis

The objective of this analytical chapter is to provide insight into cybercrime judgments rendered within the EU and at the international level. It is intended to help practitioners and offer relevant case studies and/or comparative analyses. The analysis focuses on the most interesting aspects of the case, rather than covering all issues and arguments addressed by the Court.

The analysed judgments have been selected from the court decisions that have been sent to Eurojust on a voluntary basis by the practitioners of the Member States and third States.

3.1. Selected Court rulings

Procedure: Court of Appeal, DPP v. Mark Mulligan, Ireland

Date: 18 February 2016

Keywords: interpretation of the term production of child pornography, text can constitute child pornography, requisites of search warrant

Facts

In the course of an earlier harassment investigation, forensic analysis of a suspect's computer equipment was undertaken. It uncovered images of child pornography and a photograph of his ex-neighbor's child. The neighbor was unaware that the suspect was discussing abducting and sexually abusing her young child with a like-minded individual online and that he had shared a photo of the child with that unknown person on Skype. The photo itself was not pornographic; it had been downloaded by the suspect from the IP's Facebook page. However he sent it to the unknown other via Skype, describing in graphic detail in electronic text messages how he would like to abduct and sexually abuse the three year old. Other sexual fantasies involving children were also discussed.

First Instance Court ruling

The First Instance Court convicted the suspect for production of child pornography and sentenced him to 4 years and 6 months imprisonment.

The suspect was the main contributor to the online text conversation, and was prosecuted for production of child pornography on the basis that the 1998 Act[1] includes reference to a **document** under "visual representation" in section 2(1)(a) of the Act, where it is set out that the

[1] Child Trafficking and Pornography Act 1998

definition applies "irrespective of how or through what medium the representation, description or information has been produced, transmitted or conveyed and [...] includes any representation, description [...] produced [...] by any other electronic or mechanical means [...]".

"Visual representation" is also set out in section 2 of the Act as including "any photographic, film or video representation, any accompanying sound or any **document**." Child pornography is defined as "any visual representation (i) that shows, or in the case of a **document**, relates to a person who is depicted as being a child and who is engaged in or is depicted as being engaged in explicit sexual activity."

On that definition and given the suspect's admissions as to his participation in the text conversation, the prosecution proceeded for production of child pornography. The suspect pleaded guilty to harassment and to possession in relation to the images.

The Defence case

The appellant appealed his conviction, arguing that the material in question was not *"child pornography''* within the meaning of the 1998 Act, or in the ordinary sense. Central to that contention was the suggestion that the material was not the conventional visual representation of a child being abused or engaging in sexual activity; it did not use images of children, nor did it show or suggest that any particular child had actually been abused. It was submitted that "the material might best be described as a fantasy conversation between the appellant and the other party".

The appellant maintained that he was unaware that the material was being stored within his computer and that it was never intended that it be so stored or produced or be capable of being produced into document form.

An issue was also raised in relation to the section 10 warrant used, because the Gardaí had not specified the precise offence, but had referred in the warrant to 'an arrestable offence.'

The appellant argued that he did not know he was producing child pornography, and so ought not to have been convicted of 'knowingly' producing.

Court proceedings

The Court of Appeal held that:

- ✓ Section 2 of the 1998 Act identifies the means by which such sexual activity or sexual exploitation may be conveyed, thereby bringing it within the definition in section 2 of the Act. This includes visual and/or audio representation, computer graphics, electronic or mechanical means, print publication, video recordings and film. It potentially captures almost every conceivable means of conveying information or imagery, other than, possibly, a private oral conversation between two people unheard by others and, of course, the private thoughts of an individual which are not disclosed to any third party.

- ✓ In this case, the material in question clearly constituted the storage of "data capable of conversion into a document." It is a fact that the data in question was stored in such a way that its retrieval in the form of a document was possible, and was in fact so retrieved by the investigating Gardaí. The contention that it was never retrieved by the appellant, or that he was unaware that it could be retrieved, or that he did not personally have the expertise to retrieve it in document form are all irrelevant considerations in so far as the commission of the offence in question is concerned.
- ✓ On the warrant issue crucial prerequisite for the issue of a search warrant is that *"there are reasonable grounds"* for suspecting that evidence of, or relating to, the commission of an *"arrestable offence*" is to be found in a particular place. It is not necessary that the particular offence be identified. There are many instances where the actual offence or offences may not be capable of precise identification at the point where it is deemed necessary to conduct the search of the premises. The Court referred to the earlier judgment in *Morgan* where it was said that it is desirable that the offence itself be described, but a failure to specify a particular offence will not automatically invalidate a section 10 warrant.
- ✓ Ignorance of the law is no excuse. It could be said, (and possibly reasonably and accurately in this case), that an individual who had not studied the relevant provisions of the Act of 1998 would be unaware as to what material is capable of constituting child pornography, but it cannot be suggested that such ignorance could itself amount to a defence to a criminal charge relating to the production of child pornography. The extremely graphic, sexual and violent content of the material in question, and its obvious association with young children was, by any stretch of the imagination, and irrespective of what might be contained in any legislation, pornographic and extremely so. In this case, the appellant could not but have been aware that it was pornographic, and furthermore, that it constituted child pornography in the ordinary (as compared to the statutory) meaning of that term.

Court ruling and sentence

The Supreme Court dismissed all grounds of appeal.

Thereby, this case confirms that text, including online text message exchanges, can constitute child pornography. This gives a very broad interpretation to the term 'production of child pornography' within the Irish domestic legal system.

Procedure: Supreme Cassation Court-Sezioni Unite, case no. 6889/2016, Italy

Date: 28 April 2016

Key words: admissibility of evidence gathered through remote access by LEA to device by installing virus, judicial order authorising remote access, respect for fundamental rights

Introduction

The Italian Cassation Court examined whether evidence gathered by means of interception of communications carried out through the use of viruses activated on electronic devices is allowed under Italian law and if so, under which conditions. In particular, the Court was called to determine whether interceptions carried out by installing software or "viruses" on mobile devices also require the pre-identification in the judicial order of the locations where the interception will take place. The Court also dealt with the admissibility of evidence so gathered.[2]

Facts

An order from a judge confirmed a suspect's pre-trial detention based on evidence from interception of telecommunications and witness statements attesting the suspect's involvement in extortion and drug trafficking carried out by an organised crime organisation.

The type of interception at stake is carried out by means of software (a Trojan horse) called *"captatore informatico"* or *"agente intrusore"*. This software is installed on a device (a computer, a tablet, or a smartphone) by means of email, sms or an application for software updates. This allows for the remote carrying out of a number of activities, such as:

- Interception of communication in and out from the "infected" device (internet surfing, e-mails, webmail and outlook);
- Activating the microphone thereby intercepting communications taking place in the surroundings of the suspect carrying the device;
- Using the web-camera, thereby capturing images;
- Searching the hard disk and copying in total or partially memory units of the targeted information system;
- Intercepting whatever is written through the keyboard connected to such system ("keylogger") and visualising what appears on the device ("screenshot"); and
- Avoiding anti-virus software available commercially.

The information so gathered is transmitted via internet, in real time or delayed, to the investigators' system.

The Defence subsequently filed an appeal before the Supreme Cassation Court – Sesta Sezione, against the judicial order. The Sesta Sezione remitted the matter to the Sezioni Unite of the Court for final determination.

[2] Based on this Court ruling, the Italian desk at Eurojust has made an overview of EU Member States' practice in relation to interception of communications through the use of a technical tool (virus).

The Defence case

In asking that the matter be resolved by the Supreme Cassation Court, the Defence argued, *inter alia*, that the judge's authorisation of the interception of telecommunications among people located in private places/locations through a self-installing virus should be annulled. The evidence gathered pursuant to this authorisation should be declared inadmissible.

More in detail the Defence claimed that the **order from the judge**:

- **Allowed such interception, without distinguishing between communications in public or private locations.** This would make the authorisation contrary to Article 266(2) of the Italian Criminal Procedure Code (C.P.C.) which prohibits the carrying out of interception of telecommunications in private locations, unless a criminal activity is being carried out in such premises.
- **Did not specify the locations where the interception would take place.** This would be in breach of Article 15 of the Italian Constitution and Article 8 of the European Convention of Human Rights, which protect the right to respect for private and family life, home and correspondence. According to the Defence, this argument is supported by a previous sentence of the Cassation Court (Sez. 6, n. 27100 of 26 May 2015, the so-called '*Musumeci judgement*') stating that remote interception of conversations by means of a "*agente intrusore informatico*" activated in the microphone of a mobile device is allowed only where the authorisation identifies specifically the places in which such interception will take place.

Court proceedings

The Sezioni Unite were addressed with the question **whether it is allowed to intercept conversations or communications among individuals present in private locations** according to article 614 C.P.C. - even when these places are not individually identified beforehand and even if there is no reason to believe that a criminal activity is ongoing in these places - via the installation of a 'Trojan horse' in portable electronic devices.

The Court noted that this technical means of investigation is very useful for investigations and prosecutions. It can take place anywhere; hence even within the suspect's home, remotely, without putting at risk the investigators. For these reasons, however, a balance has to be struck between the need to recourse to invasive investigative measures and the need to guarantee the respect for the individual's rights. The Court also relied on a number of legislative initiatives taken in recent years in Italy aiming at regulating the use of these devices in investigations and prosecutions of serious crimes.

The Sezioni Unite stated that the type of interception at stake falls within the category of the so-called "intercettazioni ambientali". Hence, the Court considered the matter in relation to the applicable legislative provisions, namely Articles 266, 267 and 271 C.P.C. and Article 13 of Law no. 252 of 1991 pertaining to organised crime, to ascertain whether the pre-identification of the location(s) in which the interception of communications among people present will take place is a requisite for the validity of such interception.

The Sezioni Unite further relied on previous jurisprudence from the Italian Constitutional Court to state that the Italian Constitution does not contain an absolute prohibition of interception of communications inside private locations. In addition, previous jurisprudence of the Cassation Court states that fundamental rights protected by Articles 14 and 15 of the Italian Constitution are preserved thanks to the prior judicial authorisation required for the start and modalities of the interception.

The Court then examined whether the **indication in the judicial act authorising the interception**, of the **location(s)** where such interception will take place is essential for the validity of the same interception.

The Sezione Unite stated that:

- The indication of a specific location where communications among people there present can be intercepted is not specifically provided for in Article 266(2) C.P.C., or in the jurisprudence of the European Court of Human Rights[3].
- Such indication cannot be considered a requisite for the validity of the interception; rather, it pertains to the modality in which the interception will be carried out. For instance, the Court refers to the use of "bugs" where the indication of the location in which they are placed points to the modality of the execution of the interception. If carried out by a virus in a mobile device, the technical feature of such interception does not allow to refer to any specific location, as per se this interception is "mobile" (*itinerante*).
- A special regime exists for investigations and prosecutions relating to organised crime. Article 13 of Law No. 152 of 1991 allows interceptions at the habitual residence of a suspect even if there is no reason to believe that a criminal activity is being carried out in that location. This provision expresses the intention of the legislator to favour the use of an investigative means for crimes the investigation of which can be particularly difficult. By so doing, the legislator has carried out a careful balancing of all the interests at stake, choosing for a more considerable limitation to the secrecy of communications and protection of domicile in consideration of the exceptional gravity and dangerousness for any citizens brought about by organised crime. Serious threats to society posed by complex organised crime networks ask for a strong position from the State. This means that any means modern technology can provide can be used, provided that this occurs in the full respect of current legislation and the principles enshrined in the Italian Constitution, which can be interpreted to encompass the evolution of technology.
- The *Musumeci judgement* did not consider relevant applicable provisions from which emerges a clear distinction between interceptions among people present in a given location, and interceptions between people present in private locations. The same judgement also did not consider the special regime established by Law No. 152 of 1991. For these reasons, the said judgement was in contrast with previous judgments from the Cassation Court allowing interceptions by means of "virus" in relation to proceedings on organised crime, and with previous judgments from the same Court that have always excluded the necessity to pre-define the interception-locations. Consolidated case law foresees that when the addressees and type of locations are indicated in the authorisation, the interception as such is valid.

[3] *see* Vetter v. France of 31 May 2005, Kennedy v. United Kingdom of 18 May 2010

- Regarding the case at stake (i.e. interception of communications among people present by means of a virus installed in a mobile device, in the context of investigations of organised crime) the condition is that the judge authorising such interception adequately reasons his decision to authorise the interception.
- In relation to proceedings regarding organised crime, the installation of a virus in a mobile device, authorised by a decision of the judicial authority adequately motivated and in full respect of all applicable law provisions, represents one of the "natural" ways of carrying out interceptions, the same as those carried out by bugs within a private location.
- It is not relevant that the mobile device carrying the virus can intercept conversations among people present anywhere, considering that:
  a) the indication of the location is not among the requisites prescribed by law in cases of interceptions of communication among people present in a place, with the exception of private places for which it is required by law that there are solid reasons to believe that a criminal activity is taking place in that said place;
  b) the special regime applicable to organised crime allows interceptions in private places, without requiring the solid reasons to believe that a criminal activity is taking place there.
- Regarding the jurisprudence of the European Court of Human Rights, there seems to be no incompatibility with Article 8 ECHR as interpreted by the Strasbourg Court considering that:
  a) proportionality between the intrusive nature of this technical means and fundamental rights has been respected by the legislator, in consideration of the need to protect citizens from heinous forms of crime;
  b) it is not required that the judge's authorisation of the interception indicates the locations in which interception will take place[4].

The Sezioni Unite therefore concluded that in so far as proceedings pertaining to organised crime are concerned, interceptions of communications among people present in a location by means of a "*captatore informatico*" installed on mobile electronic devices are allowed also in private locations, even though these are not singularly defined and even if no criminal activity is taking place in such locations.

Court ruling

In rejecting the Defence's arguments, the Sezione Unite of the Italian Cassation Court decided that the interception of telecommunications by means of a virus installed on a mobile device was carried out in full respect of the law and hence the evidence so gathered was declared admissible.

[4] see Zakharov v Russia, 4 December 2015, and Capriotti v. Italy, 23 February 2016

Procedure: 1st Instance - District Court of The Hague, case no. 09/767152-15, The Netherlands

Date: 21 October 2015

Key words: Phishing, malware, remote access by LEA

Facts

In September 2014 customers of a Dutch media and telecommunication services provider received phishing emails (over a number of mail runs), in which they were invited to enter into a competition to win a tablet and to click on a link in the message to visit the competition web page. By clicking on the link, the customers were redirected to a phishing website, which looked like the authentic website of the telecom provider, after which they were requested to log into their personal account. Over 150 victims entered their login credentials. By doing so, the criminals gained access to the victims' personal customer pages. With this information criminals were able to make phone calls and purchase goods at the cost of the customer. Earlier that same year, other phishing emails had been sent to customers of the same telecom company, informing them about an outstanding invoice which, if not paid, would lead to additional fees. By clicking on the attachment (fake invoice) in the email, malware containing a key logger was installed on the victim's computer.

Charges

The accused was charged with:

- Swindling (Art. 326 of the Dutch Criminal Code (C.C.)), jointly committed over a period of 10 months: inducing others to give up their login credentials for their telecom provider user accounts, by
  - sending their victims email messages wherein they presented themselves as representatives of the telecom provider and
  - luring their victims to false pages, posing as webpages of the telecom provider, with the promise of a chance to win a tablet and
  - requesting their victims to fill in their account details.
- Attempts to commit swindling;
- Co-perpetration of qualified theft: unlawful transfer of funds from PayPal accounts.
- Computer intrusion, jointly committed and/or;
  Possession of malware with the intent to commit computer intrusion, and/or;
  Installing a device capable of eavesdropping, intercepting or recording communications or data transfer: infecting their victims' computers with malware, by inducing them to open an attachment in an email message wherein they presented themselves as representatives of the telecom provider, and subsequently logging keystrokes on their victims' computers.
- Possession of computer passwords, access codes or similar data.

Evidence

The phishing mails sent out by the criminal group in the first run contained a tracking pixel, which led to a Hotmail address that was used to sign up for the telecom provider's electronic newsletter. The IP associated with that communication could be traced to a physical address. For subsequent phishing mail runs, information from the mail headers and traffic analysis by the telecom provider, led to the same IP address. Wiretap information yielded solid evidence that the user of the IP address was involved in the phishing activities, prompting the prosecutor to order the arrest of the defendant. At the time of arrest, the defendant's premises were searched. On a seized laptop, additional evidence regarding the phishing mail runs was discovered, along with malware and a file containing login credentials of several persons' online services (including PayPal accounts). This information could be linked to police reports of fraudulent transactions from compromised PayPal accounts.

Forensic analysis of the laptop yielded the login credentials of the defendant's Hotmail account. With a warrant of the investigating judge, police remotely entered the Hotmail account and preserved its contents. The analysis of the laptop also yielded login credentials of a Gmail account associated with the user of the laptop. The contents of this account were also preserved by the police, with the warrant of the investigating judge.

Court proceedings

The defence argued that a third party possibly hacked the defendant's computer and misused his IP address for criminal activity. The defence supported this alternative scenario with an expert witness report.

The Court in its ruling first established that based on several undisputed facts, it should be held that the defendant was the sole (legitimate) user of the IP address associated with the crimes for which he was charged. Secondly, the Court observed that the mail addresses that were used during the criminal activities were accessed from the defendant's laptop. The Court therefore held that the defendant had access to these mail accounts. Lastly, the Court remarked that a .txt file, containing what appeared to be the content of a phishing email, was found in a folder on the laptop that also held school reports drafted by the defendant. The Court therefore found it unlikely that defendant was a victim of computer intrusion himself.

The evidence thus showed that the computer used to commit the crimes belonged to the accused. Further proof was given to show that the accused was present at the physical address from which contacts had been made to the telecom provider. On the basis of this evidence, the accused was held guilty of phishing. The computer of the accused further contained information which revealed that his computer had been used to install malware and a key logger on the victims' computers. Based on the evidence presented, his liability for computer intrusion and for intentionally and unlawfully intercepting data was established.

Court ruling and sentence

The Court convicted the accused on all charges and sentenced him to 24 months' imprisonment, including six months of suspended prison sentence, with a three year probationary period.

The Court stressed the seriousness of the fact that the phishing offences had been committed over a period of ten months. He had also committed computer intrusion, which can potentially have very serious consequences, if the trust of the general public in the security and reliability of the Internet is undermined.

Noteworthy is that the Court also ordered the permanent confiscation (under Dutch law: the withdrawal from circulation) of a smartphone seized during the search of the defendant's premises. The Court ruled that even though the phone was locked and the police did not succeed in gaining access to the device, a smartphone offers many of the same technical functionalities as the laptop that was seized during the same search. The Court therefore held that the smartphone must have been used in committing the offences for which the Court has convicted the defendant.

Procedure: 1st Instance - District Court of Zeeland-West-Brabant, case no. 02/820936-14, The Netherlands

Date: 29 June 2016

Key words: Rovnix malware, banking malware, participation in a criminal organisation

Facts

From October 2013 to July 2014, three large Dutch banks filed complaints with the police for alleged criminal offences committed by means of banking malware. Criminals hacked into quite well-known and 'normal' websites and installed the so called 'Rovnix malware' on these sites. When unsuspecting persons subsequently visited these web pages, the computer of the visitor was infected and the malware installed unnoticed. As soon as the infected computer was used for online banking, the malware triggered a series of events which gave the criminals access to the banking details of the victim and made it possible to make money transfers from the victim's account to the accounts of money mules.

Charges

The accused was believed to have fulfilled a coordinating role in the criminal activities and was charged with:

- Theft/attempted theft;
- Money laundering;

- Participation in a criminal organisation, the aim of which was to commit criminal offences, more specifically
  - the manufacturing and/or distribution of banking malware;
  - computer intrusion;
  - theft;
  - intentionally disabling a computerised device or system of telecommunication;
  - repeated money laundering.

Evidence

On the basis of information reported to the police by the banks, such as an overview of possible fraudulent transactions and a copy of a presumed malware file, as well as investigations conducted on the computers of victims and statements made by mules, the police discovered a.o. that the HASH-values of an executable file and the C&C-server were identical; the 'webinjectcodes' found on the infected computers started with the same digits, the ATS-servers used during two separate attacks were registered under the same email address, etc. This made it possible to link the different attacks with the same malware, and the same perpetrators.

Court proceedings

The Court first explained the working mechanism of the Rovnix malware, which once installed, makes contact with a Command and Control server. This C&C server instructs the infected computer to transfer certain types of data. As soon as the victim initiates online banking, the malware makes sure that an ATS server receives all data which are shown and typed on the infected computer. This ATS server enables criminals to create new money transfers, split transfers or change the recipient of a transfer. The malware disguises the changes so that irregular transactions cannot be noticed on the infected computer. A 'human' intervention is however needed to insert the account numbers and names of recipients of the money. This is done via the entering of 'injectcodes'. These injectcodes need to be entered with each new attack, as they differ per bank and per recipient. In order to cash out the fraudulent transactions, one needs to have control over the bank accounts of these recipients.

The Court noted that owing to the efforts of the banks and their customers in stopping, pausing or undoing the money transactions, a large number of the fraudulent transactions in question had not been successful. In such cases, the offence was to be qualified as attempted theft. Where the money transfer was successful, the Court qualified the offence as theft, regardless of whether or not the money had been withdrawn from the account or transferred to another bank account. The evidence showed that the accused was engaged intensively in acquiring names and bank account numbers, possessed bank cards of third persons and presented himself as someone else in his communication with banks. He consequently also had access to the money which entered the affected accounts. It was established that the accused was aware of money being transferred to the accounts of money mules and that malware was used to unlawfully transfer money from the victims' accounts. Accordingly, the Court held the accused guilty of attempted theft and theft.

Based on the findings related to (attempted) theft, the Court concluded that the accused was aware of the criminal origin of the transferred money. To qualify as money laundering, the offence should also involve concealing the nature, source, location or transfer of the money. The evidence showed that the malware used disguised the changes made to the money transfers, which made it impossible for victims to discover the unlawful transfers. The money transfer could only be seen if the victim checked previous transactions on an uninfected computer or if the bank discovered irregularities among the transactions made. Such disguise qualified as concealment for the purposes of money laundering. As the accused was aware of the use of this type of malware and played an active role in transferring money further to second level money mules, as well as in withdrawing fraudulently transferred money from the bank accounts used, the Court found him guilty of repeated money laundering.

The Court further had to consider the participation in a criminal organisation in this specific case of cyber offences committed through the use of malware. Simple cooperation among perpetrators is not sufficient to qualify as a criminal organisation. In addition, the perpetrators need to feel bound towards the organisation and make a contribution to reach the objective of the organisation. In this case the sequence of acts needed to acquire the money, from the development of the malware to the withdrawal of money, was very complex. It required such coordination of every activity to be carried out that only a group of people, possibly divided into several levels, could achieve full implementation of the necessary acts. Therewith, the requirements of a criminal organisation were fulfilled. With regard to the accused, the evidence showed that he participated in activities that were directly linked to the realisation of the objective of the criminal organisation.

Court ruling and sentence

The accused was found guilty as charged and was sentenced to 24 months' imprisonment.

Procedure: 1st Instance - District Court of Rotterdam, case no. 10/960167-13, The Netherlands

Date: 20 July 2016

Key words: TorRAT malware, banking malware, participation in a criminal organisation

Facts

This case concerned TorRAT malware that was spread by means of so called spam runs in 2012 and 2013, with the aim of committing fraud to the detriment of customers of two large Dutch banks. Thousands of spam emails were sent to customers, reminding them of a (fake) unpaid bill, and containing a link to what seemed to be an invoice or another PDF file. By clicking on the link, the TorRAT malware was installed on the computer of the customer. This enabled the criminals to remotely manipulate the customers' online banking through a Command and

Control server. The malware subsequently made it possible to reroute money transfers that were made through online banking from the infected computer. The money was transferred to the accounts of money mules and cashed out or exchanged into Bitcoins.

Charges

The accused was charged with:

- Money laundering, by disguising the origin and transfer of money and Bitcoins received through the infection of computers with malware and online fraud; and/or
  Making use of bank accounts in the name of money mules, through which money was transferred.
- Participation in a criminal organisation, the aim of which was to commit criminal offences, more specifically the offences of
  - Computer intrusion;
  - Intentionally and unlawfully hindering the access to or using a computerised device or system by offering or sending data;
  - Installing a device capable of eavesdropping, intercepting or recording communications or data transfer;
  - Intentionally and unlawfully intercepting or recording data transferred through a computer system, by means of the use of a technical device;
  - Possession of an object which contains data which were illegally obtained through interception or recording;
  - Theft;
  - Money laundering.

Evidence

Fox-IT (a private Dutch security company), conducted investigations into the functioning of the TorRAT malware, on behalf of the victimised banks, and established that the malware is controlled by configuration files containing the bank account numbers and names of account holders (money mules) to whom the money transfers have to be made. The Court subsequently used this information as a basis for determination of causality (see below).

Court proceedings

Four main issues were considered by the Court:

The defence argued that the causality between the TorRAT malware and the bank transfers had not been sufficiently established. According to the defence, several viruses affecting banks existed at the time of the offences, and therefore it could not be established whether the specific bank transfers mentioned in the complaints filed by the banks to the police were a result of the use of TorRAT or of another virus. On the basis of Fox-IT's assessment (TorRAT controlled by configuration files containing names and bank account numbers of recipients of the money

transfers), the Court found that the transfers made to the bank accounts (of money mules) mentioned in the police reports, were in any case a direct consequence of the use of TorRAT malware. Subsequently, considering that a large number of the transfers had been made exactly to the money mules appearing in the configuration files, another cause for the fraudulent transfers than the TorRAT malware could be excluded. Contrary to the defence, the Court did not find it necessary to establish for every single transaction separately that the money transfer was caused by the malware in question. The Court, thus, found causality established.

Second, the Court examined the charge of money laundering and found that the investigation, statements of the money mules and the complaints that the banks had filed with the police, brought forward enough evidence to prove this offence. The money successfully transferred to the bank accounts of money mules was used to make payments or was exchanged into Bitcoins, either directly by the money mules or following an additional transfer to the accounts of second level money mules.

Third, the Court considered that the existence of a criminal organisation is inherent to cyber fraud as committed in this case. Activities such as developing malware, hacking into servers, spreading malware through spam runs and acquiring money mules with the aim of getting access to bank accounts, require a preconceived plan and coordination among the people involved. On the one hand the availability of the right technical insight and equipment was required. On the other hand the successful commission of this type of computer fraud required the availability of a sufficient amount of money mules who could act in a timely manner to ensure the expropriation of the money transferred from the victims' bank accounts. In view of the fact that the criminal activities were carried out over an extended period of time, the accused and others involved cooperated in a structured and sustainable manner and, thus, formed a criminal organisation.

Fourth, the Court elaborated on the concept of 'participation' in a criminal organisation, more specifically the participation by some of the criminals (technical side) in the money laundering. The accused had allegedly committed money laundering together and in association with others, labelled as co-perpetration under Dutch criminal law. The Court pointed out that emphasis should be put on the cooperation between the perpetrators rather than on the question as to who carried out which task. In this case the cooperation of the accused with others made the commission of TorRAT fraud possible. The 'technical side' and 'money mule side' require frequent and close cooperation. In such cases the money laundering is an inseparable part of the computer fraud. Considering the gainful money laundering activities in the present case, the accused and other perpetrators involved must have acted in close cooperation.

Court ruling and sentence

The Court convicted the accused of co-perpetration of money laundering and participation in a criminal organisation, aimed at committing criminal offences.

The accused was sentenced to 36 months' imprisonment and the payment of damages of 105491.42 Euro. The Court considered such punishment justified, as attacks on the online

banking system like those carried out by the accused and his co-perpetrators are grave and harmful offences that reduce the level of confidence in the integrity of the electronic payment system.

Procedure: Appeal for cassation - Supreme Court STS 10447/2015, Spain

Date: 4 December 2015

Key words: Child abuse material found on computer, absence of a reasoned judicial decision in relation to the search of the computer, right to privacy, admissibility of e-evidence

Facts

This case regards the appeal of a conviction for (i) sexual abuse and (ii) the use of children for the production of pornographic material. A woman had made, at a male friend's request, numerous videos and photos of a sexual and pornographic nature of her five year old and eight year old daughters (the victims), which were sent via skype and/or email to her friend. The child abuse material (CAM) was detected by coincidence by a technician who had been asked by the mother to repair her computer. The technician alerted the police who immediately arrested the mother. The victims' mother immediately confessed, she voluntarily gave the police the computer equipment, including the access codes, and she cooperated effectively to reveal the identity of her friend. A subsequent house search at the house of the friend was also conducted.

Both the victims' mother and her friend were convicted to custodial sentences by the Court of First Instance of Santa Cruz de Tenerife. The mother's friend (the appellant) appealed his conviction to the Supreme Court.

First Instance Court ruling and sentence

The Court of First Instance of Santa Cruz de Tenerife, convicted the victims' mother and her friend for:

- **Sexual abuse**: the victims' mother was convicted to 16 years and 8 months in total, and her friend to 22 years in total. For the victims' mother mitigating circumstances applied because of her confession and cooperation with the investigation.
- The **use of children for the production of pornographic material**: the victims' mother was convicted to a custodial sentence of 14 years in total and her friend to 16 years in total. For the victims' mother mitigating circumstances applied as above.
- Both the victims' mother and her friend were also convicted to **additional sentences**, including the loss of parental authority (victims' mother); a contact ban of ten years superior to the duration of the custodial sentence (both); a prohibition to do whatever type of child-related activities up to ten years after the execution of the custodial sentences (both); and a disqualification from passive suffrage (both).

The Defence case

The appellant contested his conviction on the following **legal grounds**:

- A breach of the **right to privacy** (Article 18(1) of the Spanish Constitution). The appellant claimed that his conviction was based on illegally obtained evidence since there was no reasoned judicial decision (no "auto judicial motivado") -and thus no check as to the adequacy, necessity or proportionality – with regard to the looking into and examination of the emails of the victims' mother during the house search at her place.
- A breach of the **presumption of innocence** (Article 24(2) of the Spanish Constitution) as a consequence of the use of illegally obtained evidence.
- An **Error of law**.

Court proceedings

The Supreme Court relied, to a large extent, on previous case law from the Spanish Constitutional Court and the Supreme Court, to support its findings that:

- ✓ The fact that the evidence was found accidentally by a technician who was in charge of repairing the computer and who alerted the police - in compliance with the legal duty that every citizen has, namely to inform the authorities when her or she becomes of a potential criminal offence - cannot lead to the conclusion that the evidence was illegally obtained.
- ✓ The fact that the evidence was gathered without a reasoned judicial decision ("auto judicial motivado") cannot lead to the conclusion that the evidence was illegally obtained, for the following reasons:
  - The mother consented voluntarily that the police had access to her computer and provided the police with the access codes which allowed them to identify numerous files containing CAM. The given "consent" was assessed and considered to be in line with the standards required by the Spanish Constitutional Court.
  - The evidence found on the computer included images and dialogues that were held in the past via programs of instant messages. There was no interception of on-going telecommunication and there was no interception of telecommunication that was concluded, but not yet received by the recipient.
  - There is a constitutional, legitimate aim that allows a restriction to the right of privacy, namely the investigation and discovery of facts of a very serious nature involving extremely vulnerable victims. The actions of the police were necessary in terms of proportionality.
- ✓ The appellant's identification data were voluntarily provided by the mother so there was no question of a breach of a constitutional right.
- ✓ The information that was provided by the telecom providers met the proportionality test.

- ✓ The mother's alleged emotional feelings towards her friend were considered irrelevant; her accusations/confessions could be taken into account as evidence.
- ✓ The alleged absence of a specific judicial authorization for the access to the appellant's electronic emails was rejected. The judicial authorization for the appellant's house search explicitly mentioned the aim of collecting any technological element which could reveal the communications held between the appellant and the victims' mother.

Court ruling and sentence

The Supreme Court found that there was no breach of Article 18(1) of the Spanish Constitution, there was no breach of Article 24(2) of the Spanish Constitution and there was no error of law. The evidence was not illegally obtained. The Supreme Court dismissed all the arguments raised by the Appellant and confirmed the 1st instance judgment of the Court of Santa Cruz de Tenerife.

The Supreme Court upheld the sentences imposed by the SAP Santa Cruz de Tenerife.

Procedure: Appeal for Cassation: Supreme Court STS 204/2016, Spain

Date: 10 March 2016

Key words: Evidence obtained through interception of mobile phones without prior judicial authorisation, right to privacy and secrecy of communications, necessity and proportionality of the measure

Facts

This case regards the appeal of the conviction of one of the appellants for drug trafficking offences based on evidence obtained through the interception of mobile phones without a prior judicial authorisation during the police investigation. The police intercepted the communications as well as the list of contacts of the mobile phones. The appellant was convicted by the Court of First Instance and appealed his conviction to the Supreme Court.

First Instance Court ruling and sentence

The appellant was convicted by the Audiencia Provincial de Sevilla on 29 May 2015 inter alia for drug trafficking. He was convicted to imprisonment of 4 years and 6 months and a fine of 75.000 Euro.

The Defence case

The appellant contested his conviction on the following **legal grounds**:

- ➢ A breach of the **right to privacy** (Article 18(1) of the Spanish Constitution). The validity of the evidence obtained was challenged on the grounds that it was obtained through the

illegal interception of communications since there was no reasoned judicial decision or order (no "auto judicial motivado"). He claimed a breach of his right to secrecy of communications.

- A breach of the **presumption of innocence** (Article 24(2) of the Spanish Constitution) as a consequence of the use of illegally obtained evidence.

Court proceedings

The Supreme Court relied on previous case law from the Spanish Constitutional Court and the Supreme Court, to support its findings that:

- ✓ Evidence obtained through the access of police investigators to mass electronic storage devices without a prior judicial authorization is not valid and cannot substantiate the conviction of the accused.
- ✓ Judicial authorization must fully abide by the principles of speciality, suitability, exceptionality, necessity and proportionality of the measure.
- ✓ Judicial authorization is needed to protect the information contained in these devices because the data stored affects the fundamental right to privacy in general, and in particular the right not to have intrusions in one's digital environment, a Constitutional right of new generation.
- ✓ The Supreme Court establishes a difference between (i) the incoming and outgoing phone calls from the mobile phones and (ii) the data contained in the list of contacts. Accessing the list of contacts of the mobile phone is not considered a breach of the right to secrecy of communications, but a breach of the right to privacy.
- ✓ Judicial authorization is always mandatory with the exception of urgent cases, where such measure is possible with a subsequent court validation.
- ✓ The breach of the right to privacy by the inquiry measure can only be justified by reasons of urgency and necessity. Moreover, it must comply with the principle of proportionality (weighting conflicting interests: the sacrifice of the right to privacy and the public interest).
- ✓ In the present case, the Supreme Court found that access by the police to the list of contacts of the mobile phones was not justified by reasons of urgency or necessity.
- ✓ It follows that evidence obtained by the police from the mobile phones without judicial authorization and absent of any reasons for urgency and necessity is not sufficient to substantiate the conviction of the accused.

Court ruling and sentence

The Supreme Court found that by proceeding to the interception of the mobile phones and accessing the list of contacts without a prior judicial authorization there was breach of the right to secrecy of communications and the right to privacy. The interception was not justified by reasons of urgency and necessity. The Court therefore upheld the appeal, confirmed that there had been a breach of the right to privacy and overturned the 1st instance judgment of the Audiencia Provincial de Sevilla.

3.2. Other Court rulings in brief

Procedure: Court of Cassation, Criminal Chambers, no. 15-82642, France

Date: 16 December 2015

A case heard by the French Supreme Court involved an investigation into drug trafficking, criminal association and smuggling offences. During the investigations, the investigating judge issued an order for the interception of encrypted instant messages exchanged between two individuals through Blackberry Messenger using the internet. Pursuant to this order, RIM company (Blackberry) was requested to deliver the unencrypted version of the messages.

Article 100 of the French Code of Criminal Procedure prescribes the rules for lawful interception of correspondence exchanged via telecommunication. The Court of Cassation in this case ruled that instant messages exchanged between several people in a secured manner by use of an encryption device constitute correspondence through telecommunications within the meaning of Article 100 of the Criminal Procedure Code and can, as such, be intercepted upon decision by and under the authority and control of a judge.

Procedure: Supreme Court case No 2K-138/2015, Lithuania

Date: 6 January 2015

This case involved a defendant who accessed, obtained and stored email correspondence from a private e-mail account of another person (victim) by using the victim's login information. The defendant subsequently sent the private correspondence to others without the victim's consent. The defendant challenged the appeal decision on a number of points.

The defendant argued that criminal liability should have been based on Article 198(1) instead of Article 1981 of the Lithuanian Criminal Code. In this respect, the Supreme Court recalled that article 1981 was adopted to criminalise illegal access to an information system as an independent criminal offence pursuant to the Budapest Convention as well as Framework Decision 2005/222/JHA and decided that Article 1981 was the correct legal basis. In support of this argument it points out that this provision criminalises access to an information system by violating its security measures. In this case, the defendant illegally entered the legitimate user's login data thereby misleading the system, which is to be considered as a violation of the security measures of the system. Consequently, the aforementioned article applies.

On a further ground of appeal, the Supreme Court decided that Article 168 of the Lithuanian Criminal Code, which criminalises the violation of a person's privacy, encompasses not only breaches of privacy in the physical, but also in the electronic environment. In the Court's view it

was this article that constituted the correct basis for prosecuting the defendant's act of sending the victim's private correspondence to others (thereby publishing it).

Procedure: Supreme Court case No 2K-188-489/2015, Lithuania

Date: 12 May 2015

In this case, the defendant had committed DDoS attacks on several (Lithuanian) websites, using software in his possession. An appeal was lodged to the Supreme Court.

One of the main bases for prosecution was Article 198²(1) of the Criminal Code which prohibits the unlawful handling of installations, software, passwords, login codes and other data as well as *inter alia* the acquisition or possession of software designed for the commission of criminal offences, adopted in line with Council Decision 2005/222/JHA. Since software and other electronic means can have both criminal and legitimate purposes (dual-use), the Supreme Court stated that it is necessary to establish a direct intention to use such tools for the commission of criminal offences. On this point, the Court overturned the appealed decision and pointed out that even though the software acquired by the defendant could have been used in a legitimate way – i.e. to test the reliability of a system – it was nevertheless used criminally, because it was acquired and kept to unlawfully access websites.

In addition, the Court dismissed an argument raised by the defence in relation to the jurisdiction of the First instance Court. The defence argued that since the damages occurred at the servers' location in Sweden, Lithuanian courts lacked competence. However, the Supreme Court dismissed the argument by recalling Framework Decision 2005/222/JHA which affords jurisdiction to the Member State where the offence was committed in whole or in part. This includes cases where the offender is physically present on its territory and, whether or not the attack is against and information system located on its territory. Since the attack was conducted in Lithuania, the First instance Court did possess the jurisdiction to hear the case.

Procedure: Supreme Court, case nr. 2016/908, Norway

Date: 30 August 2016

The Norwegian Supreme Court was addressed with the question whether the forced use of a suspect's fingerprint to access a computer, mobile phone or any other fingerprint protected device in order to gather evidence, is covered by the legislation on coercive measures.

Previously, the Appeal Court ruled that this practice is covered under Section 157 of the Criminal Procedure Act, which stipulates that "*any person who with just cause is suspected of any act punishable pursuant to statute by a custodial sentence may be* ***subjected to physical***

examination *when it is deemed to be of significance for the clarification of the case and does not amount to a disproportionate interference. Blood samples may be taken and other examinations may be carried out if they can be done without risk or considerable pain.*" The Court thereby concluded that the forced use of the fingerprint to unlock a mobile phone could be considered as being subjected to physical examination.

The Supreme Court however, in its ruling on 30 August 2016, decided that Norwegian police is not allowed to forcibly use a suspect's fingerprint in order to get access to a locked mobile phone. The Court argued that the legal instrument in question (Section 157) applied to analysis of fingerprints etc. as factual evidence, not for use in biometric locks.

The Supreme Court did not take any stance with regard to whether or not access via biometric data would be a violation of the right against self-incrimination.

3.3. Case Study: Microsoft Corporation v. United States of America

On 14 July 2016, the U.S. Court of Appeals for the Second Circuit pronounced a ruling in the case of *Microsoft Corporation v. United States of America.* An analysis of the Court ruling is presented below, followed by an outline of the relevant U.S. legal provisions in relation to disclosure of data by service providers, with a particular focus on the distinction between U.S. law enforcement and judicial authorities and non-U.S. authorities for this purpose.

3.3.1. Analysis Court Ruling

Background

Before going into the details of the case at hand, it is important to know how Microsoft Corporation (hereinafter 'Microsoft'), a U.S. incorporated and headquartered business, stores its customers' data. Content and non-content data of users of Microsoft's web-based email service - currently called 'Outlook.com'- is stored on a network of servers. These servers are divided over datacenters in different regions in the world, 'segmented' by Microsoft (for the E.U. region, servers are located in Dublin, Ireland). Microsoft generally stores *content data* of its customer's emails and accounts at the datacenter which is located closest to the physical location which the user identified as its place of residence when subscribing to the email service. Microsoft does not verify the correctness of the information provided by the user when subscribing to the service. Only some limited *non-content data* (such as basic account information, including user name and country, as well as transactional data) is retained within the U.S., regardless of the location of the user.

Facts and legal provisions

In December 2013, a magistrate judge in the District Court for the Southern District of New York issued a warrant on the government's application, having found probable cause to believe that an email account was being used for the purpose of narcotics trafficking. The warrant, served on Microsoft at its headquarters in Redmond, ordered the search of a specific email account which was controlled by Microsoft, as well as the disclosure of content of emails, subscriber information, traffic data and records pertaining to communications with MSN and any person regarding the said account. The warrant requested this data for the period of creation of the account to the date the warrant was issued.

Microsoft subsequently disclosed the information which was stored within their U.S. data storage facilities, but determined that the requested content data was exclusively stored in its datacenter in Ireland and consequently filed a motion to quash the warrant with respect to the user content data. Microsoft reasoned that warrants traditionally carry territorial limitations, and therefore their authority only extends to locations within the U.S., but does not reach further -outside U.S. territory. The magistrate judge however denied quashing the warrant, by arguing that the warrant provisions in the SCA entail similar obligations as those of a subpoena to "produce information in a service provider's possession, custody or control regardless of the location of that information". The judge therefore concluded that Microsoft was obliged to produce the customer's content data, wherever it might be stored.

The magistrate judge's decision was upheld in appeal. Not long after, Microsoft was held in civil contempt for refusing to comply fully with the warrant.

The Stored Communications Act (SCA) under the Electronic Communications Privacy Act (ECPA)

The ECPA was introduced in 1986 in order to address interception of computer and other digital and electronic communications. Title II of the ECPA was enacted as the Stored Communications Act (SCA). The SCA protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers. The SCA was enacted to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment. It imposes general obligations of non-disclosure on service providers and creates several exceptions to those obligations (Sections 2702 and 2703). Section 2703 establishes conditions under which the government may require a service provider to disclose the contents of stored communications:

- Pursuant to §2703(c)(2), *basic subscriber and access logs* can be obtained simply with an administrative subpoena. For such an administrative subpoena, probable cause does not need to be demonstrated.

- *Other non-content records (transactional data)* can be obtained by a court order (a '§2703(d) order') or warrant[5].
- In general, for disclosure of *contents* of electronic communication, a search warrant is required, which should demonstrate probable cause that the account will contain the evidence, fruits or instrumentalities of the crime under investigation.[6]

§2703 calls for warrants issued under its purview to be issued "using the procedures described in the Federal Rules of Criminal Procedure", which refers to rule 41 on search and seizure. This rule describes the territorial reach of federal warrants, mostly limited to a particular federal judicial district. It also allows magistrate judges to issue warrants that may be executed outside the issuing district, but still within another district of the U.S.

Court proceedings

In order to come to a conclusion in this case, the U.S. Second Circuit Court of Appeal had to assess whether the District Court relied on a mistaken understanding of the law in issuing its order, as well as whether the denial to quash a motion rested on a mistake of law. For that purpose, it mainly based its reasoning on an **analysis of the SCA,** with its legislative history, and referred to the principles set forth by the Supreme Court in ***Morrison v. National Australian Bank Ltd.***[7]

On analogy to the approach followed in *Morrison v. National Australian Bank Ltd.*, the Court proceeded in two parts:

(1) It first determined whether the relevant provisions encompass extraterritorial application.
(2) It then assessed whether the challenged warrant had, in fact, extraterritorial effect.

(1) The (extra)territorial reach of the warrant under the SCA

The Court began by analyzing Congress' intention, when enacting the **warrant provisions of the SCA**, regarding the provisions' reach. When interpreting the laws of the U.S., the Court presumed that legislation of Congress is meant to apply only within the territorial jurisdiction of the U.S., unless there is a clear indication of a contrary intent.[8] The SCA is silent as to the (territorial) reach of the Act as a whole and as to the reach of its warrant provisions in particular. Section 2703 in particular, does not mention any extraterritorial application either. In the absence of an affirmative indication of an extraterritorial reach, Congress clearly did not intend for the SCA warrants to have effect outside U.S. territory, the Court ruled.

[5] 18 U.S.C. §2703(c)(1)
[6] 18 U.S.C. §2703(a) and §2703(b)(1)(A)
[7] Morrison v. National Australian Bank Ltd., 561 U.S. 247 (2010)
[8] So-called 'presumption against extraterritoriality'

Moreover, the Court stated that the use of the term "**warrant**" by Congress, also emphasizes the domestic boundaries of the Act in these circumstances. The warrant is an instrument by which the power of government is exercised and constrained; it appears in the Fourth Amendment to the U.S. Constitution. As the term is used in the Constitution, it is traditionally linked to the protection of U.S. citizens' privacy interests and applied within the territory of the U.S. Accordingly, a warrant protects privacy in a distinctly territorial way.

The Court then proceeded by examining the government's and District Court's view that an SCA warrant is equivalent or closer to a **subpoena** (which is not territorially limited) than a traditional warrant (which is limited in its scope as described above). The Court however, reasoned that Section 2703 of the SCA clearly distinguishes between a warrant and a subpoena, to distinguish between a greater or lesser level of protection of stored communications. Consequently, the Court ruled, there is no reason why Congress would use 'warrant' to mean 'subpoena'. The Court also addressed the government's argument that a subpoena (and similarly a SCA warrant) may require the production of materials which are located outside the U.S. The Court refuted the argument, based on case-law, by clarifying firstly, that a subpoena with extraterritorial reach can only be enforceable when it is addressed to a foreign individual whose acts outside of U.S. jurisdiction (intend to) produce detrimental effects within the U.S. In such a case, the individual would indeed be compelled to hand over the requested materials. Secondly, the Court concurred with Microsoft's observation that it merely holds records on behalf of a customer, who has a protectable privacy interest in the item and that there is a difference between requesting a company to hand over its own documents, and requesting it to hand over someone else's documents.

- ⇨ Based on these preceding arguments, the Court concluded that Congress did not intend the SCA's warrant provisions to apply extraterritorially.

The Court also briefly elaborated on the **focus of the SCA**, which it found to be primarily on the need to protect a user's privacy interests in electronic communications, and not on a presumption of law enforcement access to content. Disclosure is therefore permitted only as an exception to the primary obligation to protect a user's privacy. According to the Court, Congress also enacted the SCA with the aim to ensure that the privacy protections which American citizens enjoyed for 'traditional' forms of records or communications were also extended to the electronic forum. Law enforcement needs were therefore not the primary motivator for the enactment.

(2) Extraterritoriality of the warrant served

Based on the user privacy focus of the SCA, the Court concluded with relative ease that the execution of the warrant would constitute an unlawful extraterritorial application of the SCA. Considering the data subject to the warrant was exclusively stored at, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the U.S. Microsoft would indeed have had to interact with its Dublin datacenter to retrieve the information, and the data lied within the jurisdiction of a foreign state. The Court acknowledged that the current process for obtaining foreign-stored data through mutual legal assistance

procedures is cumbersome, but in the Court's view these practical considerations cannot overrule the focus of the SCA, its other aspects, legislative history and the meaning and reach of a 'warrant'. This led the Court to conclude that an SCA warrant may reach only data stored within U.S. boundaries.

- ⇨ Thus, to enforce the warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the SCA.

Court ruling and conclusion

Based on the foregoing arguments, the Court concluded that the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a U.S.-based service provider for the contents of a customer's electronic communications stored on servers located outside the U.S. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's email account stored exclusively in Ireland. Microsoft therefore had no remaining lawful obligation to produce materials to the government.

Therefore, the Court:

- ⇨ Reversed the District Court's denial of Microsoft's motion to quash;
- ⇨ Vacated the District Court's order holding Microsoft in civil contempt of court;
- ⇨ Remanded the case to the District Court, with instructions to quash the warrant insofar as it demands the user content stored outside of the U.S.

3.3.2. Analysis U.S. provisions on disclosure of data by service providers

Under Title 18 Section 2702(a) of the U.S. Code, providers of public electronic communication services (ISPs and over-the-top providers) and providers of remote computing services (hosting providers and over-the-top providers) are prohibited from divulging any information they hold for their customers, as well as information about their customers and the use of their services. Certain exceptions are allowed, as described in the statute. Disclosure of data may occur on the basis of **voluntary cooperation** by the provider (18 USC § 2702(b) and (c)) or on the basis of a **legal requirement** to do so (18 USC § 2703).

For the purpose of **required disclosure** to U.S. governmental authorities, U.S. law recognises three categories, described in the analysis of the judgment above: (1) via administrative subpoena, for *basic subscriber information (BSI) and access logs*, (2) via production order for *transactional data* and (3) via a warrant for *content data*. With the exhaustive listing of what is considered to be BSI under 18 USC § 2703(c)(2) and the practical clarity what constitutes content data, whatever data is *not* considered BSI or content, may be considered *transactional data*. This would include traffic data, but also information regarding the volume of communications and possibly email header information. The acquisition of data from providers for the purpose of MLA takes place on this same statute.

For the purpose of **voluntary disclosure**, U.S. law only distinguishes between *content data* and *customer records or other information pertaining to a customer* (what would typically be called metadata), although providers, in their policies for voluntary disclosure, may differentiate between BSI and transactional data.

The disclosure of content data is regulated under 18 USC § 2702(b), whereas the disclosure of metadata is regulated under 18 USC § 2702(c). Subsection 6 of the latter statute allows disclosure of metadata to *any person other than a U.S. government entity*. It is this provision that enables the voluntary disclosure of non-content data to non-U.S. law enforcement and judicial authorities[9]. As a practical consequence, U.S. law enforcement and judicial authorities can obtain less data through voluntary disclosure than their foreign counterparts.

The regime for voluntary disclosure of content data is stricter than that for metadata and limited to certain situations. For non-U.S. law enforcement and judicial authorities voluntary disclosure of content data is typically limited to exigent circumstances (or as the statute states: "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency" (18 USC § 2702(b)(8)). This is commonly referred to as *emergency disclosure*.

The ruling of the Second Circuit Court of Appeals does not regard the voluntary disclosure of data and therefore does not impact the existing practice of direct cooperation between US-based providers and non-U.S. law enforcement and judicial authorities. The core of the ruling is that it limits the coercive effect of required disclosure on the basis of 18 USC § 2703 to data which is located (stored) in the U.S. (or rather, the Court of Appeals holds that the legislator never meant required disclosure under the statute to have a coercive effect beyond U.S. territory).

The practical effect of the ruling is that the so-called *data hosting location* is recognised as a relevant and explicit factor in required disclosure under U.S. law. In order to establish whether a subpoena, production order or search warrant (either for the purpose of a domestic investigation or for the purpose of MLA) can be issued to target specific data, authorities may now need to show that that data is stored within U.S. territory. How this specifically translates to the practicalities of obtaining data from U.S.-based providers is currently being mapped out. Eurojust has already provided guidance to the EU Member States in this matter and will continue to do so where required.

[9] 18 USC § 2711 states that the term *government entity* pertains to "a department or agency of the United States or any State or political subdivision thereof".

4. Topic of Interest

Remote access to a computer system - legislative landscape

This section provides a general and factual overview of the legal landscape in relation to the possibilities for LEA to remotely access a computer system. The inherently linked considerations regarding the effects of such remote access on a person's rights, such as the right to privacy, as well as the highly debated subject of the legitimacy of extraterritorial access to such data, are outside of the scope of this section and will therefore not be touched upon.

For the purpose of this section, a questionnaire on 'remote access to computer systems' was distributed to the experts of the European Judicial Cybercrime Network, as well as experts from Norway, Switzerland and the United States.[10] The experts were requested whether remote access to a computer system by law enforcement authorities (LEA) for the purpose of criminal investigations is permitted in their country. Distinction was made in relation to the location of the accessed data; between remote access to data within the domestic territory, abroad or where the location of the data is unknown.

Remote access to data or a computer system within the country

The majority (20) of the respondents indicated that it is possible in their country to remotely access data or a computer system which is located on their territory. In most countries, the legal framework provides for this possibility, whereas in some other, in the absence of specific regulations, it can be assumed that it would be possible within the existing legal context, although admittedly in some countries there is no practice or jurisprudence yet on the matter. Only six respondents replied that remote access to a computer system, irrespective of its location, is not permitted in their country. In one of these countries, a public inquiry is however ongoing, to see if the law should be changed in this respect.

Some respondents indicated that *legitimate access* to data is not dictated by the location where the data is *stored*, as long as the computer system through which the data is accessed is located within the country.

Remote access can be covered by general as well as special legal provisions. In many countries, the general rules on search and seizure are applied when LEA conduct remote searches and -possibly- seize electronic data. Almost half of the respondents did indicate having special legal provisions governing this investigative measure, be it specific rules on extended network searches, legal provisions on accessing a computer from a distance using a technical tool, or both.

[10] Out of 31 recipients, 26 replied to the questionnaire

This investigative tool can only be used upon an order of a judicial authority (judge or prosecutor). In some countries, recourse to remote access is subject to certain conditions. It can for instance only be applied in cases concerning specific and/or serious forms of crime or when there are reasonable grounds of suspicion that traces or evidence of a criminal act might be found on the device. Specific conditions sometimes also apply to the handling of the accessed data. Indeed, in some countries, the data may only be copied and not -or only in exceptional cases- removed from the source computer. Practically all countries replied that remote access can be used for the purpose of evidence collection.

Remote access to data or a computer system when its location is unknown

Out of the 20 countries which replied that remote access is indeed possible in their country, 16 indicated that this is or would also be allowed when the location of the data is unknown. Some countries indicated that, given the absence of any indication of the location of the remote computer system, they would act under the assumption that the system was located within the country. Several countries did point out that this practice had not yet been tested in court. Two countries said it is unclear whether the use of the investigative tool would be allowed in this case; in one country, it would not be allowed, as it is an essential requirement to positively establish territoriality.

As to the relevant legal provisions, all countries referred to the same provisions as the ones applicable in case of remote access to data or a computer system located within the country.

Remote access to data or a computer system located abroad

Most countries need to proceed via mutual legal assistance procedures and international cooperation before being able to remotely access computer systems abroad. Some countries did indicate that they can legally gain remote access to a computer system abroad. However it should be noted that it is not clear from these countries' replies, whether such investigative measures entail prior recourse to MLA procedures.

The countries, who replied positively to this particular question, stated that the legal provisions applicable to remote access within the country are or could be applied by analogy in this situation. Belgium has a specific provision in its Code of Criminal Procedure, explicitly allowing remote access when the data is not stored on Belgian territory. In this case, the data can only be copied and the investigating judge, via the public prosecutor's office, has to immediately inform the Ministry of Justice, which in turn informs the involved state, if this state can reasonably be determined.[11]

The table on the next page gives an overview of the relevant legal provisions per country. The provisions in green represent specific provisions on extended search on a computer system; the provisions in orange represent specific provisions for remote access by using a technical tool.

[11] Art. 88ter §3 Belgian Code of Criminal Procedure

COUNTRY	LEGAL PROVISIONS
Austria	§§110,111, 119, 120 Code of Criminal Procedure (access to seized device)
Belgium	Art 88ter Code of Criminal Procedure
Bulgaria	Section V Criminal Procedure Code; Special Intelligence Means Act; Electronic Communications Act
Croatia	Art. 257 Criminal Procedure Act (search of movable property - extended search)
Estonia	§91 and §126 Code of Criminal Procedure (search, seizure and surveillance provisions)
Finland	Chapter 8 Section 27 Coercive Measures Act Chapter 8 Sections 20, 21 Coercive Measures Act Chapter 7 Section 2 Coercive Measures Act
France	Art. 706-102-1 to 706-102-9 Code of Criminal Procedure
Germany	Sections 94 and 98 Code of Criminal Procedure (seizure, computer-assisted search) Section 110 ss 3 Code of Criminal Procedure
Greece	/
Hungary	Art 149 Act of Criminal Procedure (general provisions allowing extended search)
Ireland	Surveillance Act 2009
Italy	Art. 244.2 Code of Criminal Procedure (permitting 'searches in information systems, including by technical means')
Latvia	Provisions on search and seizure
Lithuania	Art. 158 and 159 Code of Criminal Procedure (provisions on special investigative methods)
Netherlands	Art. 125j Code of Criminal Procedure Art. 125i to 125o Code of Criminal Procedure Proposal for new provision Art. 126nba Code of Criminal Procedure
Norway	New Sections 216 o) and 216 p) Criminal Procedure Act (specific provisions on remote access awaiting parliamentary approval)
Poland	Art 236a Code of Criminal Procedure (search and seizure provisions)

Portugal	Art 15, number 5 Cybercrime Law
Romania	Art. 138 Criminal Procedure Code Art. 168 Criminal Procedure Code
Slovak Republic	Sections 10, 90, 114-116 Code of Criminal Procedure (Computer data collection within criminal proceedings)
Slovenia	/
Spain	Art. 588 sexies c. Criminal Procedure Act Art. 588 septies a. Criminal Procedure Act
Sweden	Public inquiry ongoing in view of possibly changing the law
Switzerland	Art. 246 Code of Criminal Procedure (search and seizure provisions)
United Kingdom	Common law (stored computer data) Regulation of Investigatory Powers Act 2000 (real time collection traffic data) Police Act 1997 Part III (content interception)
United States	General search and seizure provisions; Title 18 U.S.C., Section 2510 *et. seq.* and Section 3121 *et.seq.* (intercepting communications)

Green	Specific provision on extended network search
Orange	Specific provision on remote access using a technical tool

5. The Way Ahead

The Cybercrime Judicial Monitor will be distributed during the *European Judicial Cybercrime Network Kick-off meeting* scheduled to take place on 24 November 2016. It can also be accessed on the restricted website of the future European Judicial Cybercrime Network.

The focus of future issues of the CJM will be kept on the legislative developments in the area of cybercrime and the analysis of relevant court decisions. The topic of interest will be determined at a later stage, based on ongoing or emerging trends.

Importantly, the content of the CJM depends on the input of practitioners. We therefore kindly encourage practitioners to send, throughout the year, relevant national legislative developments, court decisions and other information considered useful for the purpose of future issues of the CJM to Eurojust.

We would like to thank the experts of the European Judicial Cybercrime Network for their valuable contributions they provided for this CJM.

Eurojust November 2016

Catalogue number: QP-AG-19-002-EN-N
ISBN: 978-92-95084-00-1
ISSN: 2600-0113
DOI: 10.2812/86148